*Dear Sir/Madam*

During this investigation I have conducted a report to help ensure safer passwords for you in the future, these are the findings:

1. To defend the passwords they used a MD5 hashing algorithm, this is very weak and provides little defence from attacks. I would recommend to use a different hashing algorithm such as Argon2 or SHA-256, as they will provide more sufficient security to your passwords against brute force attacks.

2. Password hashing algorithms can provide a high level of security depending on the type used, MD5 is based off a block cipher which is a one way compression function. This makes it very inefficient and not up to date in today’s world against hackers.

3. In the future using an algorithm such as Argon2 would be more beneficial, this is because it utilised cryptographic salt. Argon2 is also known to make the time of hacking a lot longer, giving you more time to call for help during an attack.

4. From my investigation I can tell that the organisation used a password policy of: a minimum length of 12, no re-usable passwords, a mix of lowercase/uppercase/numbers and account lockouts every few failed login attempts.

5. If I was to create a password policy I would make it mandatory to have: 2 factor authentication, employ a 3rd party company to ensure the passwords safety, require longer length passwords with a minimum length of 15 and no similar passwords to previous ones or any other information.

Regards,

Ben Robson